Beech Hill School E-Safety Policy

Revised September 2016

'Learning without Limits'

HEADTEACHER Mrs S Hussain

Background and Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The risk of radicalisation
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Policy and leadership

This section begins with an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with Computing. It also outlines the core responsibilities of all users of Computing in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of Computing

Responsibilities: e-safety coordinator

Our e-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e-safety coordinator: Sofia Loreen

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Provides training and advice for staff
- Liaises with school Computing technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Reports regularly to Senior Leadership Team
- Receives appropriate training and support to fulfil their role effectively

Responsibilities: governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor.

Responsibilities: head teacher

• The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator

• The head teacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. See flow chart on dealing with e-safety incidents – below and relevant Local Authority HR / disciplinary procedures)

Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

• They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

• They have read, understood and signed the school's Acceptable Use Policy for staff

• They report any suspected misuse or problem to the E-Safety Co-ordinator

• Digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems

• E-safety issues are embedded in the curriculum and other school activities.

Responsibilities: COMPUTING technician

The Computing Technician is responsible for ensuring that:

• The school's Computing infrastructure is secure and is not open to misuse or malicious attack

• Users may only access the school's networks through a properly enforced password protection policy

• Shortcomings in the infrastructure are reported to the Computing coordinator or head teacher so that appropriate action may be taken.

• Has responsibility for blocking / unblocking internet sites in the school's filtering system / passing on requests for blocking / unblocking to the Computing Helpdesk

• Maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices

Schedule for development / monitoring / review of this policy

The implementation of this e-safety policy will be monitored by the:	E-safety coordinator
Monitoring will take place at regular intervals:	Annually
The governing body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	October 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Calderdale Safeguarding Children board e-safety representative West Yorkshire Police

Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school Computing systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Acceptable Use Policies

All members of the school community are responsible for using the school Computing systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable use policies are provided in Appendix 1 of this policy for:

• Pupils (EYFS + KS1 / KS2)

• Staff (and volunteers)

• Parents / carers (including permissions to use pupil images / work and to use Computing systems)

• Community users of the school's Computing system

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents.

For children in EYFS and KS1 parents may sign on behalf of their children

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the schools Computing resources (including the internet) and permission to publish their work. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each year.

Community users sign when they first request access to the school's Computing system. Induction policies for all members of the school community include this guidance.

Self-Evaluation

Evaluation of e-safety is an on-going process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers …) are taken into account as a part of this process.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows: Core COMPUTING policies
Computing Policy How Computing is used, managed, resourced and supported in our school

Other policies relating to e-safety

Anti-bullying	How our school strives to eliminate bullying – link to cyber bullying
PSHE	E-Safety has links to this – staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms a part of the school's safeguarding policy
Behaviour	Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

• **Child sexual abuse images** (illegal - The Protection of Children Act 1978)

• **grooming, incitement, arrangement or facilitation of sexual acts against children** (illegal – Sexual Offences Act 2003)

• **Possession of extreme pornographic images** (illegal – Criminal Justice and Immigration Act 2008)

• **Criminally racist material in UK – to stir up religious hatred** (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)

• pornography

• promotion of any kind of discrimination

• promotion of racial or religious hatred

• threatening behaviour, including promotion of physical violence or mental harm

• any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on Computing kit provided by the school:

• Using school systems to run a private business

• Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school

• Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions

• Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)

• Creating or propagating computer viruses or other harmful files

• Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet

• On-line gambling and non-educational gaming

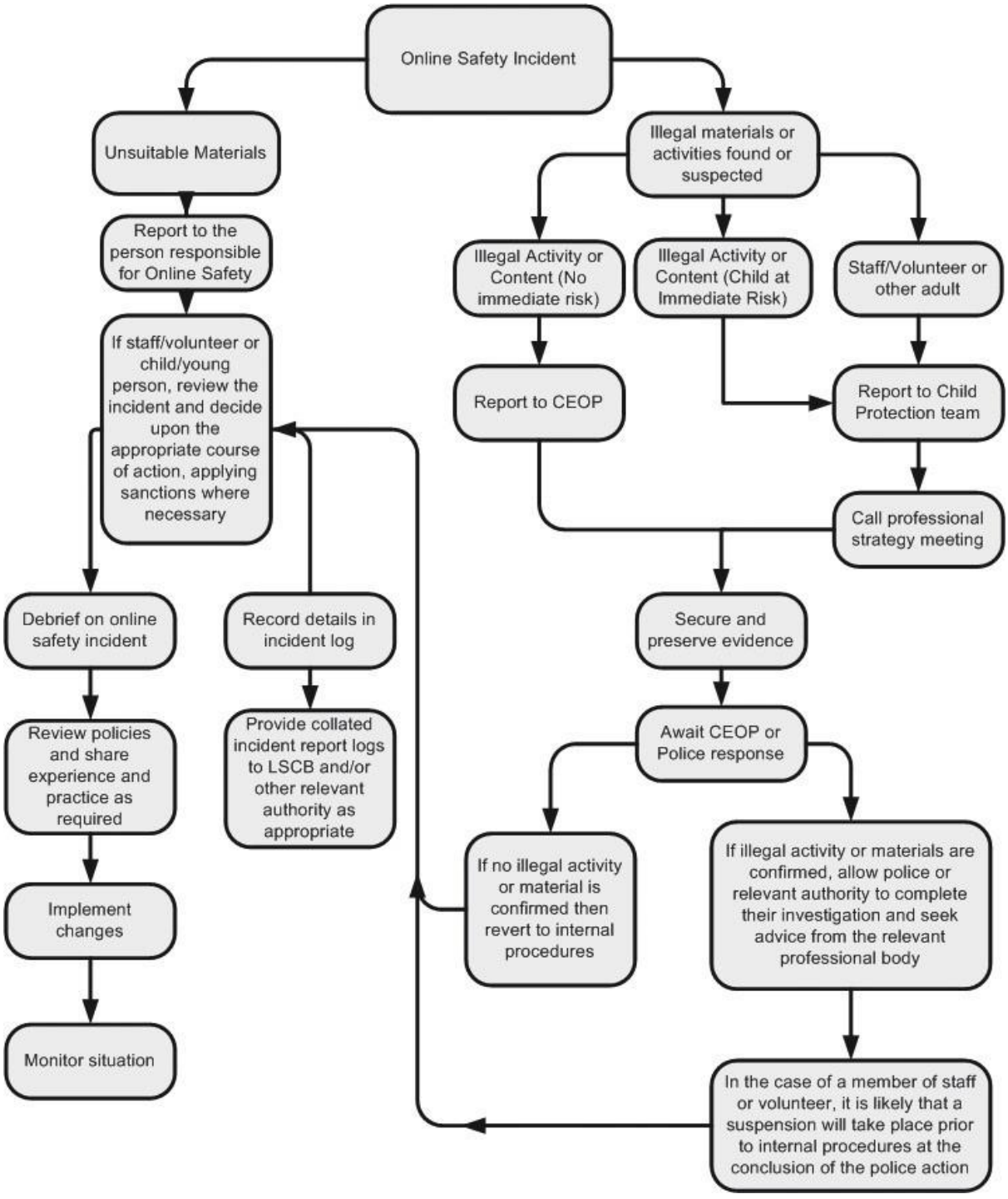
• Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of Computing, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:



Audit / Monitoring / Reporting / Review

The E-Safety coordinator will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the head teacher / and a governor on a termly basis.

Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

• Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:

- Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
- Members of staff are free to use these devices in school, outside teaching time, where children are not present, e.g. staffroom.
- Pupils are not currently permitted to bring their personal hand held devices into school.

Email

Access to email is provided for all users in school via the intranet page accessible via the web browser (Internet Explorer) from their desktop.

These official school email services may be regarded as safe and secure and are monitored.

• Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access).
• Users need to be aware that email communications may be monitored
• Pupils have access to an individual email account for communication within school.
• A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
• Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (these may be blocked by filtering).
• Users must immediately report, to their class teacher / e-safety coordinator – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section for guidance on publication of photographs

Use of web-based publication tools

Our school uses the public facing website, http://www.beechhillschool.co.uk/site/ for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

• Personal information should not be posted on the school website and only official email addresses (Provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).

• Only pupil's first names are used on the website, and only then when necessary.

• Detailed calendars are not published on the school website.

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:

o Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs

o Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

• Pupil's work can only be published with the permission of the pupil and parents or carers.

Virtual Learning Environment (VLE)

Class teachers monitor the use of the VLE by pupils regularly in all areas, but with particular regard to messaging and communication.

Staff use is monitored by the administrator.

User accounts and access rights can only be created by the school Computing Manager. Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to the VLE.

When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive. b) The material will be removed by the site administrator if the user does not comply.
c) Access to the VLE for the user may be suspended.
d) The user will need to discuss the issues with a member of SLT before reinstatement. e) A pupil's parent/carer may be informed.

A visitor may be invited onto the VLE by the Computing Manager following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf . Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content.

• These communications may only take place on official (monitored) school systems.

• Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Filtering Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the Computing Technician (with ultimate responsibility resting with the head teacher and governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Herefordshire school filtering service must:

• Be logged in change control logs

• Be authorised by a second responsible person prior to changes being made (this will normally happen anyway, as part of the process and will be the class teacher who originally made the request for the change).

All users have a responsibility to report immediately to class teachers / e-safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering /security systems in place to prevent access to such materials.

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through:

• signing and agreeing the internet and mobile telephone usage as part of the staff handbook (See Appendix 1)

• Briefing in staff meetings, training days, memos etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e- safety awareness sessions / newsletter etc.

Monitoring

• No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

Audit / reporting

Logs of filtering change controls and of filtering incidents are made available to:

- The headteacher
- The e-safety governor

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e- safety provision. Children and young people need the help and support of the

school to recognise and avoid e- safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

• A planned e-safety programme should be provided as part of Computing, PHSE and other lessons and should be regularly revisited – this will cover both the use of Computing and new technologies in school and outside school

• We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Cafe at KS2)

• Learning opportunities for e-safety are built into the Computing curriculum and are used by teachers to inform teaching plans.

• Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises. (E safety awareness day, electing an E safety ambassador council etc)

• Pupils should be encouraged to adopt safe and responsible use of Computing both within and outside school.

• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

• Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Information literacy

• Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

o Checking the likely validity of the URL (web address)
o Cross checking references (can they find the same information on other sites)
o Checking the pedigree of the compilers / owners of the website
o See lesson 5 of the Cyber Cafe Think U Know materials below

• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

• Pupils are taught how to make best use of internet search engines to arrive at the information they require

• We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Cafe at KS2)

The contribution of the children to e-learning strategy

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

Pupils play a part in monitoring this policy.

Staff training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.

• It is expected that some staff will identify e-safety as a training need within the performance management process.

• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction

• The E-Safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority, the Calderdale Safeguarding Board and others.

• All teaching staff has been involved in the creation of this e-safety policy and are therefore aware of its content

• The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.

Governor training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in Computing, e-safety, health and safety or child protection. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority (Governor Services or Learning and Achievement Service), National Governors Association or other bodies.

• Participation in school training / information sessions for staff or parents

The e-safety governor works closely with the e-safety coordinator and reports back to the full governing body

Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

• Letters, newsletters, web site, VLE

• Parents' evenings

• Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

Wider school community understanding

The school will offer family learning courses in Computing, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

APPENDIX 1: Guidelines for Internet and Mobile Telephone Usage
This policy covers all school employees.

Introduction

E-mail, the internet and mobile telephones enable staff to have more ready access to information and colleagues. They transform the way we do our jobs and can enrich the working environment.

They are therefore something to be mentioned and used whenever and wherever possible to streamline communication.

The following "traffic light" system has been produced to help staff make effective use of these technologies:

Red (Do not engage in these activities)

- Use e-mail to engage in gossip
- Make libelous statements about individuals or other organisations
- Make statements purporting to represent the school or the council when they are personal views
- Make derogatory remarks or express derogatory opinions about the school or the council
- Knowingly infringe copyright or intellectual property rights
- Knowingly send or receive anything which is illegal or fraudulent
- Knowingly send or receive material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress
- Use the facility to pursue personal business interests, for gambling on for political purposes not directly related to your job.
- Allow anyone else to use your user name and password to gain internet access.
- Knowingly engage in any activity, which threatens the integrity or availability of the school's systems.
- Attempt to break into (HACK) any area.
- Allowing mobile phones to ring during working time

Amber (Seek your manager's approval prior to engaging in the activity)

- Opening and/or sending personal e-mails in working time
- Personal purchases of goods and services via the internet in working time
- Use mobile telephones to receive or make / send personal calls or text messages in work time

Green (Legitimate use)

- Communicate by e-mail or mobile phone on behalf of the school or as an aid to pursuing tasks within the employees job remit
- Conducting research into work related matters
- Personal research of the internet or sending personal e-mails outside working hours
- Personal purchases of goods and services via the internet outside working hours
- Opening personal e-mails outside working time
- Receive/sending personal text messages outside working time
- Receiving/making personal calls outside working time

This list is neither exclusive nor exhaustive if you are in any doubt about where you should be using the facility for a particular purpose – consult a member of the Senior Management Team.

Please note that any failure to comply with the policy may constitute gross misconduct and could lead to disciplinary action. If you inadvertently access a site that contains illegal or offensive material, please inform the ICT manager immediately.

APPENDIX 2: Pupil Permissions

Name of Child: _____ Class: _____

Parental Permission Document

We would be grateful if you could complete the authorisation document below, and sign and date.

(Please tick)	Yes	No
Local Area Walks: I give permission for my child to take part in local outings during school time. This may involve transport, in which case parents will be notified.		
Sports Activities: I give permission for my child to take part in all inter-school sports activities. This will include them being transported too and from the vent (parents will be informed 2 days before the event if their chid is taking part)		
Photographs: I give permission for my child to be individually photographed or videoed where the pictures are to be displayed in school or for personal use.		
School website: I give permission for my child's image to be displayed on the schools website (photographs of children will not be displayed with their name of any personal details).		
Videos: I give permission for my child to be photographed, filmed or videoed by the media (e.g. press or television) and for the child's name to be released for publication such that he/she might be identified as an individual or as part of a small group.		
Medical: I give permission for the school to seek medical advice and provide medical treatment in the event of an emergency and/or being unable to contact me.		
Internet Access (responsible use of the internet): As part of pupils work across the curriculum and the development of pupils' ICT skills, we are providing the children with supervised access to the Internet including e-mail facilities. *Our school access provider operates a filtering system that restricts access with inappropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are in place to reduce the chances of children accessing inappropriate materials, the school cannot be help responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.*		

Signed (parent/ guardian: _____